Threats and Countermeasures

Lecture 06: Persistence

COMP-5830/-6830
Spring 2025

Per-Startup Kali Config

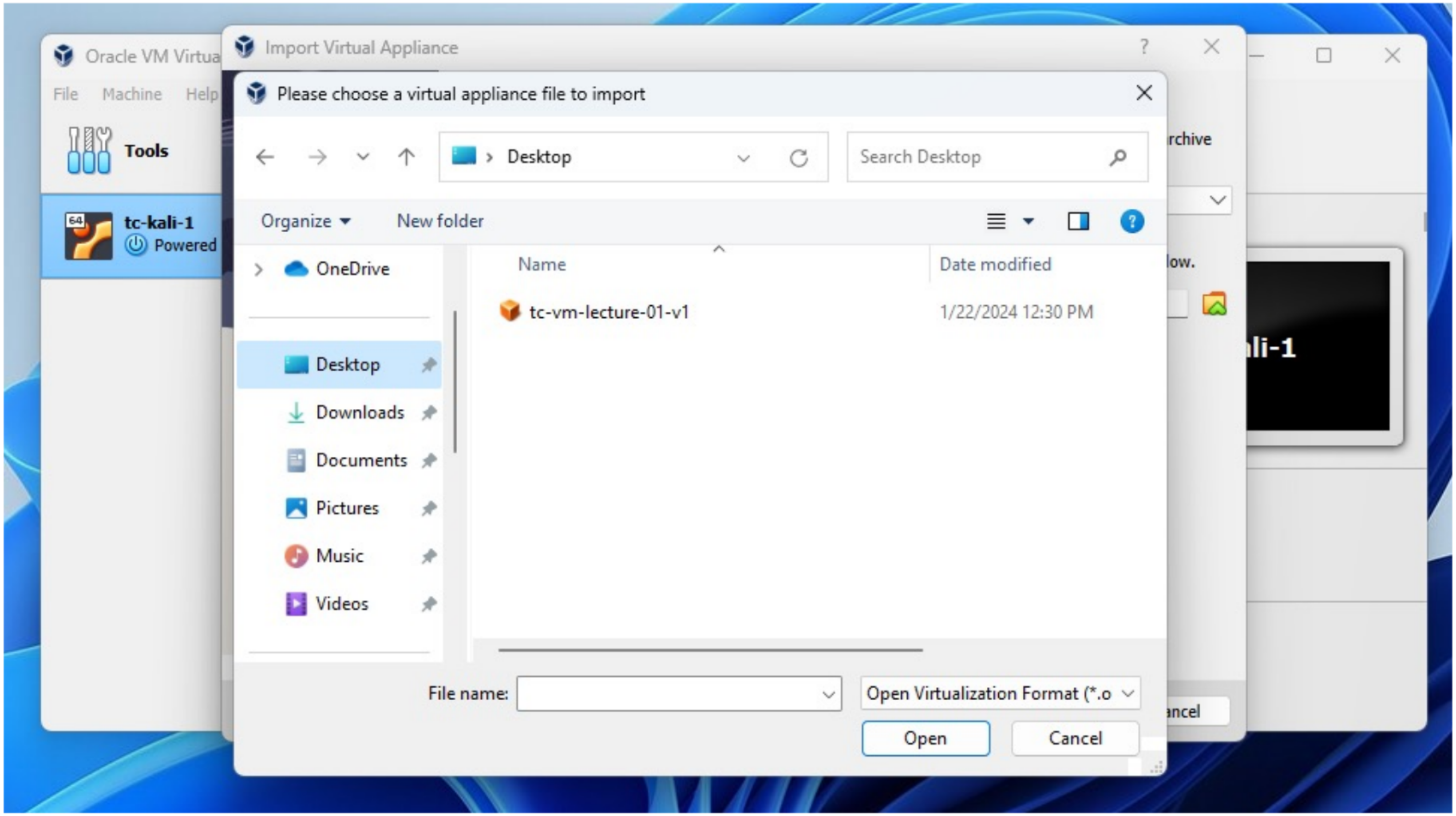
When connecting to the local VM, have to setup Kali networking ***every time you boot***.

-
  ```
  ifconfig eth0 down
  ```
  - Stop auto-detect

-
  ```
  ifconfig eth0 192.168.66.XXX netmask 255.255.255.0
  ```
  - Set Kali VM’s IP address

-
  ```
  ip route add 192.168.66.0/24 dev eth0
  ```
  - Tell Kali how to route to imported VM (1x only)

Today: tc-vm-04_rc08



Import Virtual Appliance

Please choose a virtual appliance file to import

Desktop

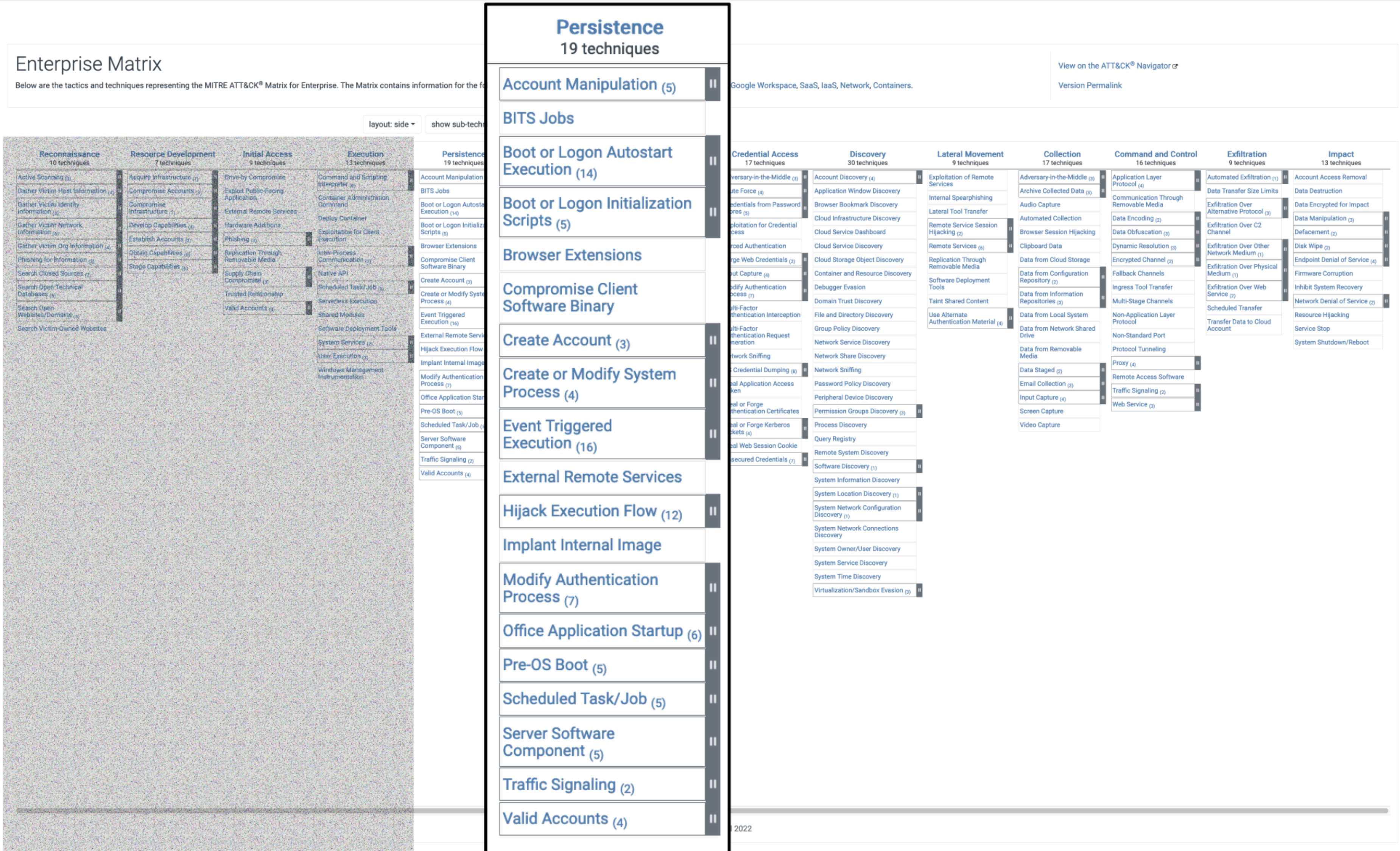
Name	Date modified
tc-vm-lecture-01-v1	1/22/2024 12:30 PM

File name:

Open Virtualization Format (*.o

Disk Crypto: bPCFDFiX32nt9zSTiWonZRsm

MITRE ATT&CK



Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the f Google Workspace, SaaS, IaaS, Network, Containers.

View on the ATT&CK® Navigator

Version Permalink

Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (7)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
13 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (7)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Credential Access
17 techniques

- versary-in-the-Middle (3)
- ute Force (4)
- edentials from Password ores (5)
- ploitation for Credential cess
- rced Authentication
- rge Web Credentials (2)
- ut Capture (4)
- dify Authentication ocess (7)
- lti-Factor thentication Interception
- lti-Factor thentication Request neration
- twork Sniffing
- Credential Dumping (8)
- eal Application Access ken
- eal or Forge thentication Certificates
- eal or Forge Kerberos kets (4)
- eal Web Session Cookie
- secured Credentials (7)

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (2)
- Web Service (3)

Exfiltration
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

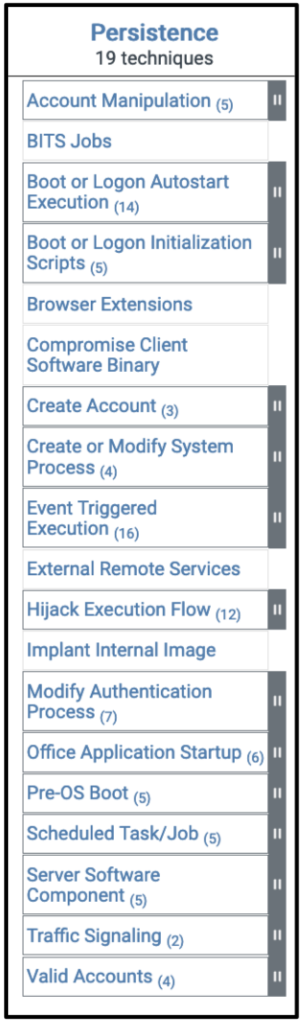
Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

2022

Persistence

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

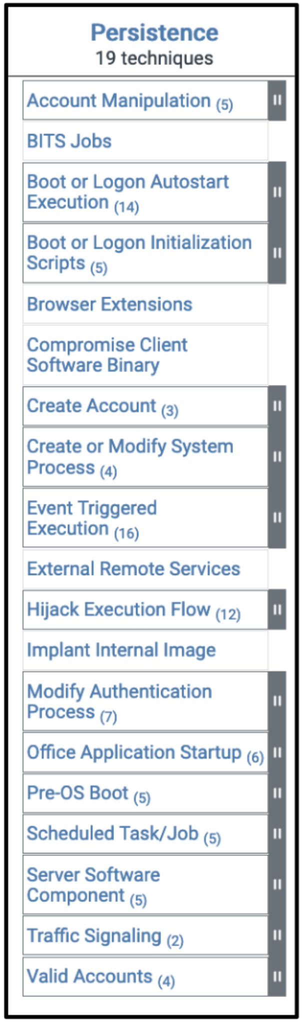


Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (7)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Persistence (simplified)

- Retain access to target systems
- Maintain a foothold across restarts, account changes, etc.



Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (7)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Account Creation

Idea: Just create an attacker account as if it were a standard user account

- Local, domain, cloud, etc.
- *Innocuous*: “alice”, “bob”, “charlie”, etc.
- *Look-a-Like*: “allce”, “Bo8”, “charles”, etc.

Account Manipulation

- Modify existing creds and/or permissions
  - Bypass defenses, change security policies, access domain acct.
- Delegate Permissions
  - Email delegates, email forwarding, etc.
- Subsume Unused Roles
  - (cloud-specific usually)
- Create Alternative Credentials
  - SSH Authorized Keys

SSH Authorized Keys

The **`authorized_keys`** file contains the public keys associated with a user and used to authenticate access.

- Usually at `~/.ssh/authorized_keys`
- If attacker-controlled public key can be added, attacker can simply log-in as that user and gain shell-access

Pre-Boot Execution

Idea: Attacker’s code runs before user has logged-in and before OS defenses running.

- Modify BIOS or UEFI firmware to ensure continued access
- Modify other firmware for other components
- Modify early-boot procedures to add/change behavior

On-Boot Execution

Idea: Attacker’s code runs after OS is available but before user has logged-in.

- Windows: via Group Policy
  - Run: `gpedit.msc`
- Linux (old): Create init.d service
  - `/etc/init.d/`
  - Configure via `update-rc.d`
- Linux (new): Create systemd service
  - `/etc/systemd/system/`
  - Configure via `systemctl`

On-Login Execution

Idea: Attacker's code runs after user has logged-in but before gaining control.

- Shell environment configs
  - `.bashrc`, `.zshrc`, `.bash_profile`, etc.
- Windows Startup Apps:
  - Run: `shell:startup`

Scheduled Tasks

Idea: Just use the same built-in capabilities from Execution phase but for different purposes

- Windows – schtasks (CMD), ScheduledTasks (PowerShell), Task Scheduler (UI)
- Linux – cron, crontab, systemd

“Traffic Signaling”

Idea: Use *arbitrary tricks* at the network-level make it difficult to detect entrance vectors.

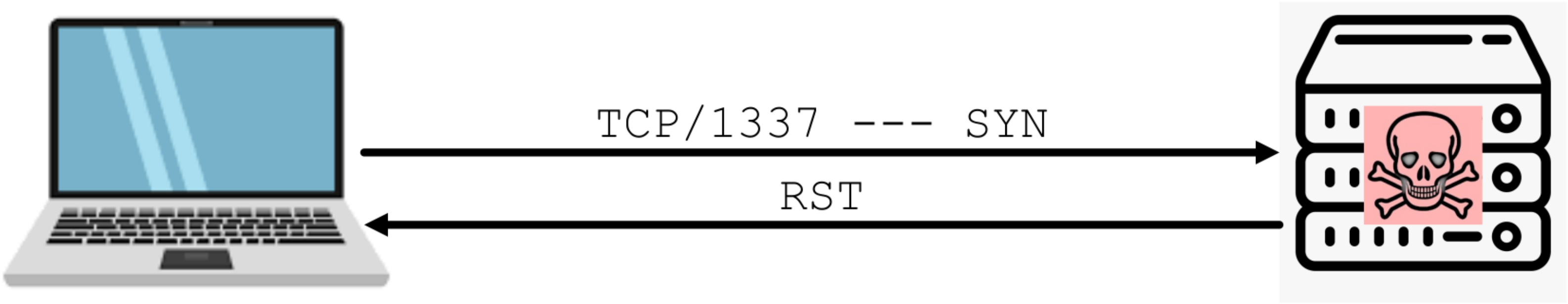
- Open ports are at risk of discovery using well-known approaches :-(
- Standard protocols can be easily noticed by IDS, IPS or human :-(

Port Knocking

Idea: Have a non-obvious trigger to open a listening port.

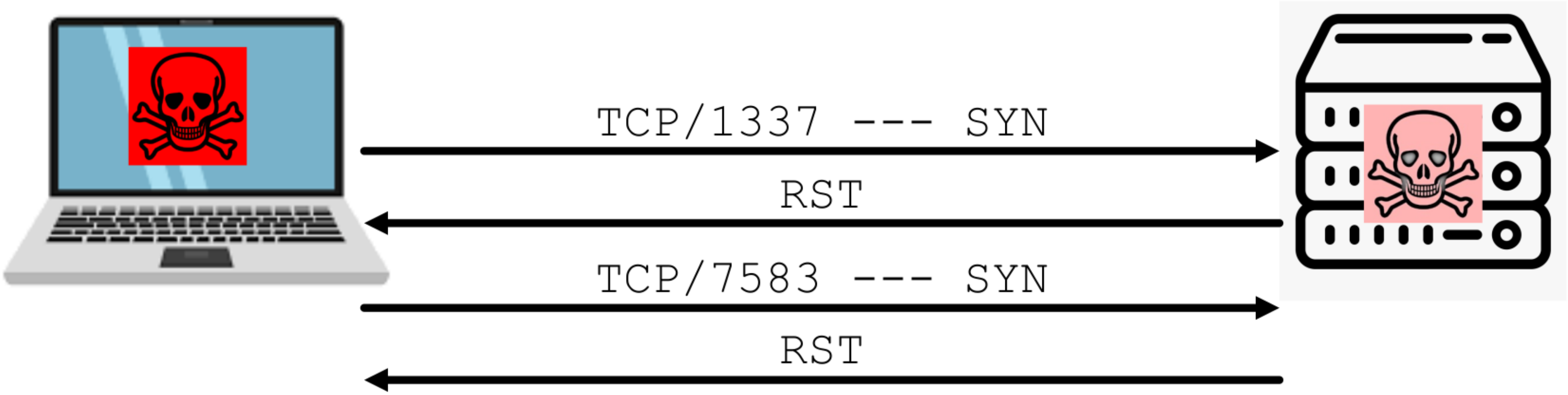
Port Knocking

Idea: Have a non-obvious trigger to open a listening port.



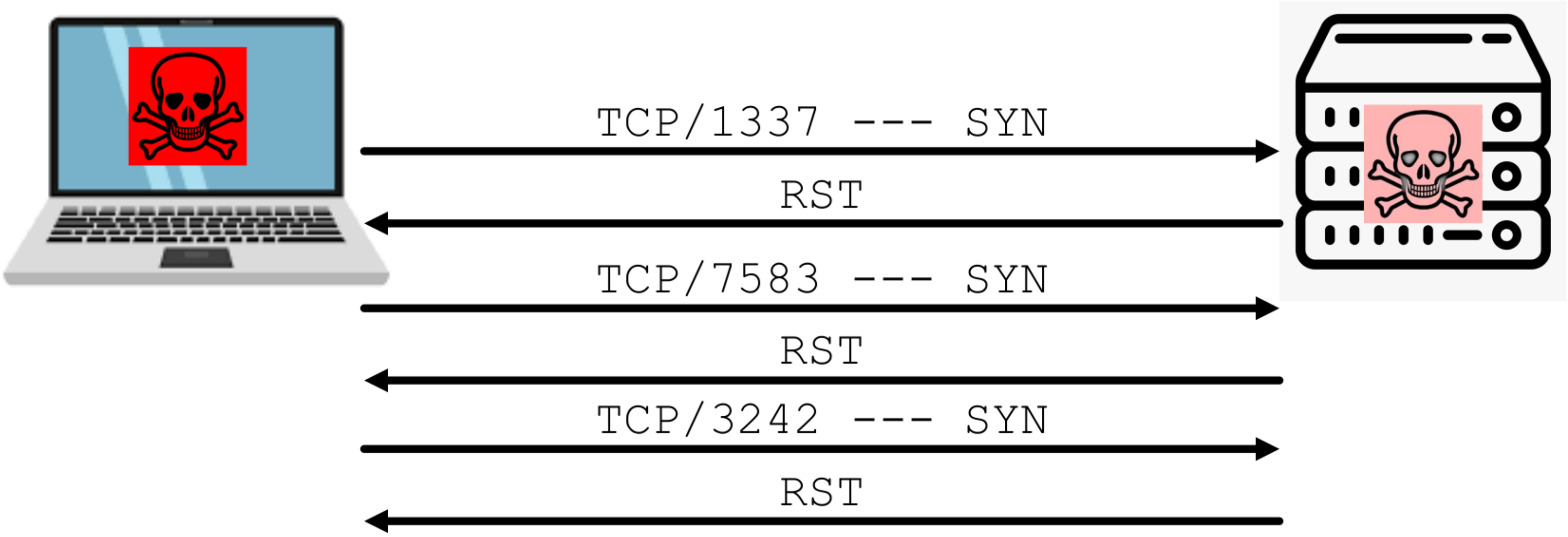
Port Knocking

Idea: Have a non-obvious trigger to open a listening port.



Port Knocking

Idea: Have a non-obvious trigger to open a listening port.



TCP/1337 --- SYN

RST

TCP/7583 --- SYN

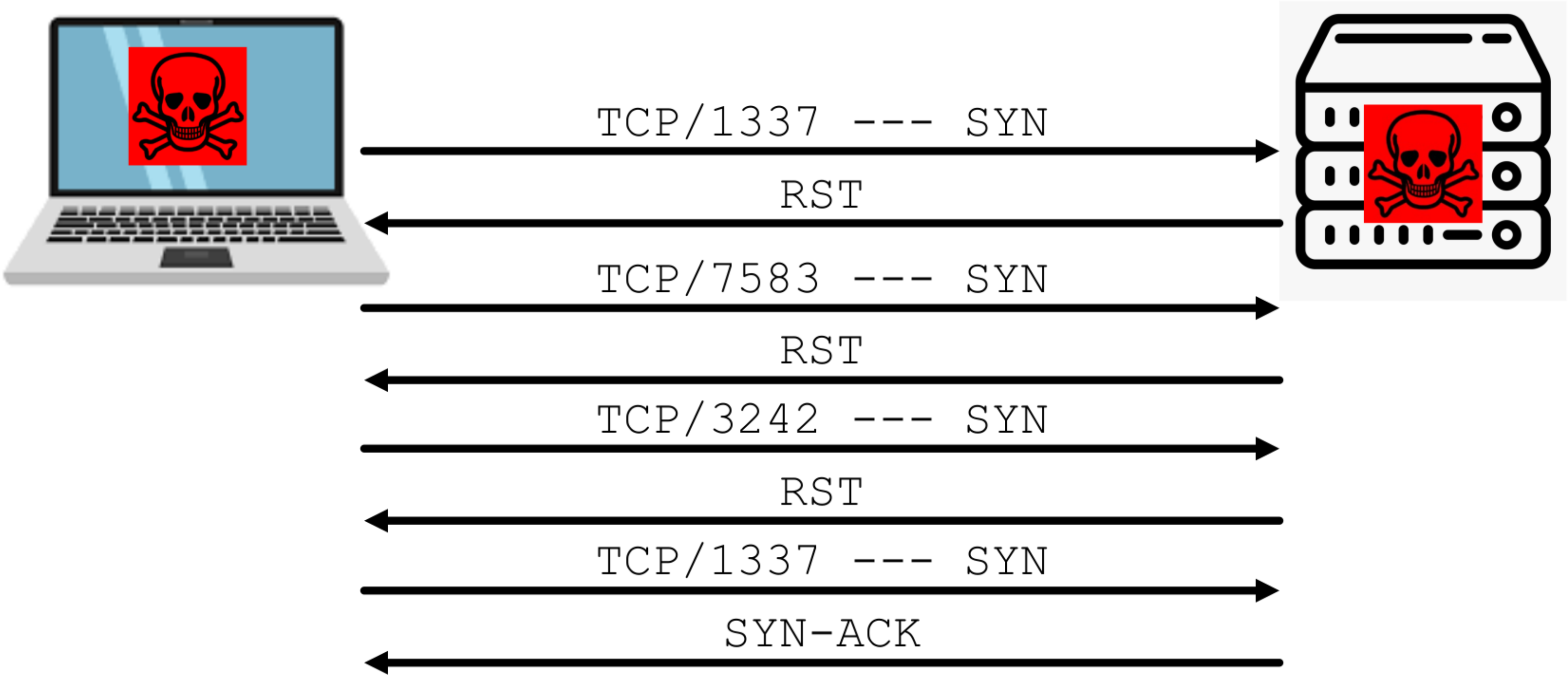
RST

TCP/3242 --- SYN

RST

Port Knocking

Idea: Have a non-obvious trigger to open a listening port.



TCP/1337 --- SYN

RST

TCP/7583 --- SYN

RST

TCP/3242 --- SYN

RST

TCP/1337 --- SYN

SYN-ACK